Säkerhetsaspekter i IEEE 802.11

Matheos Mattsson

Kandidatavhandling

Handledare: Kristian Nybom

Informationsteknologi

Fakulteten för naturvetenskaper och teknik

Åbo Akademi

Referat

IEEE 802.11 är en samling standarder för trådlöst Ethernet som ofta benämns i vardagligt tal som ”wifi”. Användningen och tillgängligheten av IEEE 802.11 har ökat i takt med att internet blir mer och mer tillgängligt för alla. Vi har idag en stor del av våra personliga uppgifter tillgängliga online och vi hanterar en hel del känsliga dokument och information via nätet. Att hantera alla dessa uppgifter så säkert som möjligt är ett måste, och för att kunna göra det behöver man insikt i hur säkerheten över anslutningen man använder fungerar.

Denna avhandling redogör för vad IEEE 802.11 är och vilka potentiella säkerhetsproblem dess användning medför. Den tar även upp allmänt om kryptering och attacker. Slutligen går den igenom hur man kan gå till väga för att hålla sig så säker som möjligt när man använder sig av IEEE 802.11.

Innehåll

1 Introduktion

IEEE 802.11 är en samling standarder för trådlöst Ethernet, men i vardagligt tal använder man ofta ordet ”wifi”. IEEE 802.11 blir allt mer vanligt i dagens moderna samhälle. Vart man än reser eller går är sannolikheten att få tillgång till IEEE 802.11 väldigt stor. En undersökning som gjordes i december 2018 visade att i hela världen använde sig 4,1 miljarder personer av internet [1], en siffra som stiger och stiger i takt med att internet blir allt mera tillgängligt. En stor del av dessa användare använder sig antagligen av IEEE 802.11 för att koppla upp sig till internet. Man kan på sätt och vis säga att dagens samhälle är beroende av IEEE 802.11, inte bara på grund av hur viktigt internet är för att samhället ska fungera men också på grund av enkla orsaker. Till orsakerna hör till exempel att många av de mobila enheter som används i dag inte ens har ett så kallat RJ-45 uttag som krävs för att använda sig av en trådbunden internetanslutning [2]. Det leder till att användarna endast har två alternativ kvar: IEEE 802.11 eller mobila nätverk, och ofta är det IEEE 802.11 som är den primära källan hemma och på jobbet. IEEE 802.11 började komma in på konsumentmarknaden år 1999 när ett flertal företag tillsammans skapade en icke-vinstdrivande organisation vars mål var att möjliggöra den bästa möjliga användarupplevelsen oberoende av tillverkare, genom att använda en ny sorts trådlös teknik [3]. Ända sedan dess har IEEE 802.11 växt och förbättrats och blir allt mer och mer tillgänglig för alla världen över.

Även om IEEE 802.11 var ett välkommet tillskott till det moderna samhället så för den också med sig en hel del nya säkerhetsproblem och risker som tidigare inte fanns när man endast använde sig av trådbundna nät. Offentliga IEEE 802.11 nätverk blir idag allt vanligare i till exempel kaféer, shoppingcentrum och restauranger. Vi som användare kanske tycker dessa är trevliga tillskott eftersom vi kan koppla upp oss även när vi inte är hemma utan att använda vår mobila dataanslutning men dessa är också de mest sårbara nätverken och risken att utsättas för olika attacker och cyberstölder är mycket högre än när man använder sitt egna privata IEEE 802.11 nätverk hemma. Alla med tillgång till nätverket har också tillgång till en hel del information om de andra användarna som är inloggade på nätverket, och med rätta kunskaper och verktyg kan i princip vilken person som helst få tag på en hel del information så som bilder, användarnamn och lösenord som skickas mellan åtkomstpunkten och dess användare [4].

Denna avhandling kommer att behandla risker som användning av IEEE 802.11 medför samt hur man kan förbättra säkerheten när man använder sig av IEEE 802.11, både hemma och på publika nätverk. Avhandlingen tar förutom säkerhetsaspekterna även upp en överblick av IEEE 802.11 standarden på ett allmänt plan och allmänt om hur kryptering kan förbättra säkerheten vid användning av IEEE 802.11 och olika typer av attacker som man kan bli utsatt för om man inte är försiktig.

2 Överblick av IEEE 802.11 standarden

2.1 Historia

802.11 är en familj standarder för trådlösa lokala nätverk som utvecklades av en arbetsgrupp på Institute of Electrical And Electronics Engineers (IEEE) [5].

I [6] berättas om utvecklingen av IEEE 802.11. Följande stycken om IEEE 802.11s historia är baserade på denna källa. År 1980 skapades projektet 802 av IEEE och sedan dess har många olika arbetsgrupper bildats under det. Den första specifikationen av IEEE 802.11 publicerades 1997 av arbetsgruppen 802.11. Denna specifikation klarade ursprungligen endast av datahastigheter på 1 eller 2 Mb/s på 2,4GHz-bandet och använde sig av endera frekvenshoppning (eng. *frequency hopping spread spectrum*, FHSS), infraröd (IR) eller direkt sekvens (eng. *direct-sequence spread spectrum*, DSSS). Efter ett tag delade man upp 802.11-gruppen i två: 802.11a och 802.11b. 802.11a blev en standard för IEEE 802.11 som opererade på en frekvens om 5GHz medan 802.11b blev den traditionella 2,4GHz-standarden. År 1999 introducerade 802.11b kompletterande inkodning (eng. c*omplementary code keying*, CCK) som möjliggjorde datahastigheter på upp till 11 MB/s för 2,4GHz-tekniken. Parallellt utvecklades ortogonal frekvensdelningsmultiplex, (eng. o*rthogonal frequency-division multiplexing*, OFDM) för 802.11a som i sin tur öppnade upp för hastigheter upp till 54 Mb/s.

I början av 2000-talet ansågs 5GHz-bandets höga radiofrekvenskostnad vara ett problem och därför användes standarden inte så allmänt som förväntats. Även om 802.11a inte riktigt hade funnit fotfäste ännu så blev användningen av 802.11b allt populärare och kravet på högre dataöverföringshastigheter än 11 Mb/s växte. För att kunna uppnå samma hastigheter på 2,4GHz-bandet som man tidigare bara uppnått på 5GHz-bandet, det vill säga 54 Mb/s, så implementerade arbetsgruppen 802.11g år 2002 samma fysiska lager och specifikation för mediaåtkomstkontroll (eng. *media access control*, MAC) som tidigare bara funnits i 802.11a-standarden.

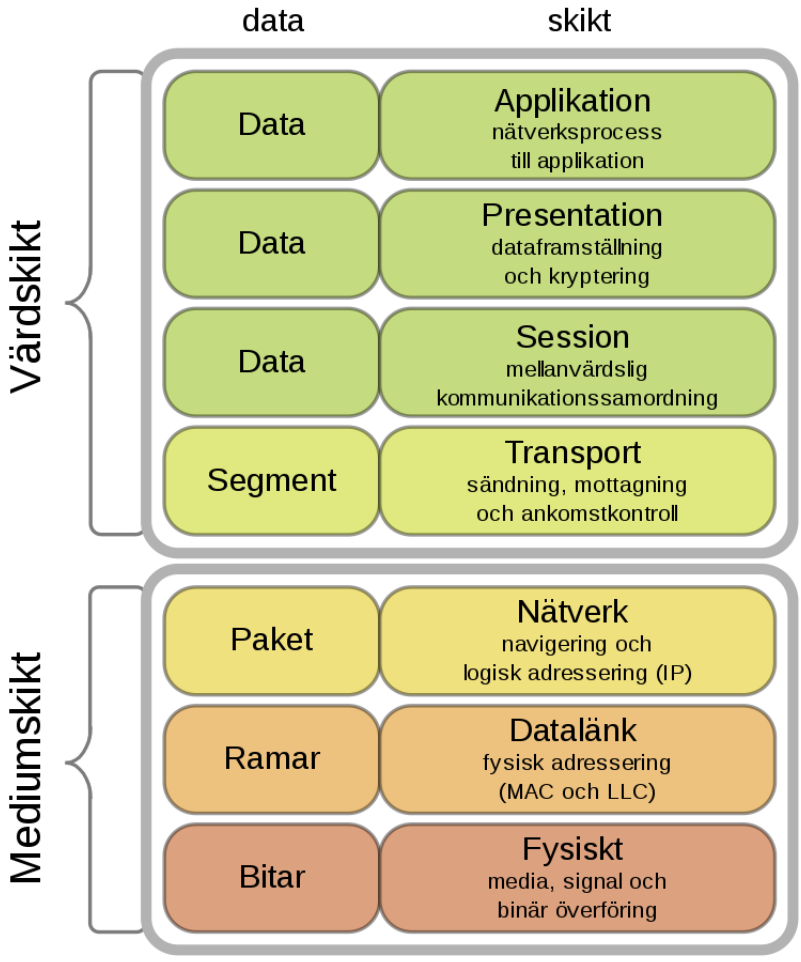
Med den väldiga ökningen av internetanvändning och användning av IEEE 802.11 fanns en konstant efterfrågan på teknik med högre dataöverföringshastigheter. Som svar på denna efterfrågan bestämde sig IEEE 802.11-kommittén att skapa ännu en arbetsgrupp, 802.11n-gruppen, för att ta fram en ny teknik som skulle stöda så kallad hög genomströmning (eng. *high throughput*, HT). Målet för 802.11n var att

uppnå en genomströmning vid MAC-lagret på 100 Mb/s. För att uppnå detta mål använde 802.11n sig bland annat av MIMO (eng. *multiple-input multiple-output*). 802.11n standarden blev klar år 2009.

5GHz-standarden utvecklades också vidare och blir i dagsläget allt mera vanlig i moderna routrar och stöds av allt fler mobila enheter. Studiegruppen för mycket hög genomströmning (eng. *very high throughput*, VHT) utvecklade MIMO-metoderna vidare genom att lägga till ett flertal mer avancerade tekniker som tillsammans möjliggjort nätverksgenomströmning högre än 1 Gb/s.

2.2 IEEE 802.11 i OSI-modellen

802.11 är inte enbart trådlös teknik utan det består av ett flertal olika protokoll som opererar på datalänklagret och det fysiska lagret i den standardiserade OSI-modellen (Open System Interconnection) som togs fram 1977 av ISO (International Standards Organization) [7]. OSI-modellen åskådliggörs nedan i figur 2.1.



Figur 2.1: OSI-modellen [8]

2.2.1 Det fysiska lagret

Det lägsta lagret i modellen är det fysiska lagret vars uppgift bland annat är att konvertera bitströmmar till olika typer av signaler (beroende på det medium som data skall skickas i), som sedan kan skickas till mottagaren som i sin tur kan konvertera signalen tillbaka till en bitström som kan läsas av exempelvis en dator. När man gällande IEEE 802.11 pratar om signaler menar man radiovågor som färdas i luften som skickas till exempel från en router eller ett modem. Det fysiska lagret ansvarar alltså för att skicka och ta emot information i form av bitströmmar från punkt A till punkt B. Det är med andra ord det fysiska lagret som kontrollerar hårdvaran och styr olika hårdvaruegenskaper så som spänningsförändringar, dataöverföringshastighet, timing av spänningsförändringar, maximala överföringsdistanser och fysiska anslutningar till överföringsmedia. Det fysiska lagret ansvar dessutom för felkorrigering, synkronisering, multiplexering (hur signaler delas in i så kallade kanaler) och frekvensmodulering [7].

2.2.2 Datalänklagret

Datalänklagret är det andra lagret i modellen och beskrivs i detalj i [7] som i dessa stycken används som referens. Dess uppgift är att kontrollera kommunikationen mellan de intilliggande lagren, det vill säga mellan nätverkslagret och det fysiska lagret. Dessutom är lagret också ansvarigt för att upprätthålla förbindelsen mellan två värdar, så som till exempel mellan två datorer. Datalänklagret hanterar ordningen av bitar till och från segment av data och organiserar mottagna data och data som skall skickas, till och från så kallade ramar. Ramarna innehåller en mängd organiserade data som erbjuder ett konsistent sätt att sända bitar över ett medium. Utan användningen av ramar skulle mottagaren av data inte kunna tolka vad som tagits emot eftersom det inte finns något sätt att säga i vilken ordning eller på vilket sätt bitarna som mottagits skall tolkas. Lagret hanterar också den fysiska adresseringen samt synkroniseringen av datapaket.

En annan viktig uppgift som datalänklagret har är att det kontrollerar flödet, vilket betyder att det kontrollerar timingen av sändning och mottagning av data så att det inte överskrider de begränsningar som den fysiska anslutningen sätter upp. Om fel uppstår på det fysiska lagret är det datalänklagrets uppgift att förmedla felmeddelanden.

Närverksenheter som opererar på detta lager är switchar och hubbar.

Datalänklagret delas in i två underlager: logisk länkkontroll (eng. *logical link control*, LLC) samt mediaåtkomstkontroll (eng. *media access control*, MAC).

Det är LLC lagret som kontrollerar synkronisering samt flödet och förmedlandet av felmeddelanden för datalänklagret (som nämnt tidigare). LLC lagret hanterar anslutningsorienterade överföringar vilket betyder att mottagaren bekräftar varje paket som tas emot och ifall ett paket försvinner ber mottagarens LLC att få det försvunna paketet skickat på nytt varpå sändarens LLC skickar om alla paket från och med det försvunna paketet. På det viset kan man garantera att alla paket kommer fram och att de kommer fram i rätt ordning. Förutom anslutningsorienterade överföringar kan detta lager också hantera anslutningslösa överföringar.

MAC lagret har hand om den fysiska adresseringen. Varje nätverkskort har sin egna unika MAC adress som också kallas för dess fysiska adress. MAC adressen, som ofta är permanent inbränd i skrivskyddat minne, används för att unikt identifiera ett specifikt nätverkskort på nätverket. MAC lagrets uppgift är att sköta om överföringen av paket från ett nätverkskort till ett annat (en MAC adress till en annan) över ett delat överföringsmedium så som IEEE 802.11.

2.3 Protokollsviten TCP/IP

TCP/IP kallas ofta för ”Protokollsviten TCP/IP” (eng. *TCP/IP protocol suite*) eftersom det faktiskt inte bara består av de två protokollen TCP och IP som nämns i namnet, utan också av en del andra sammanhängande mindre protokoll. TCP/IP är en global standard för värd-till-värd transport över internet och det opererar på transport- och nätverkslagret i den ovannämnda OSI-modellen [9].

TCP/IP är inte en samling protokoll som är specifikt för IEEE 802.11 utan det används också av trådbundna anslutningar men dess vikt är så pass stor för avhandlingen att det ändå bör tas upp.

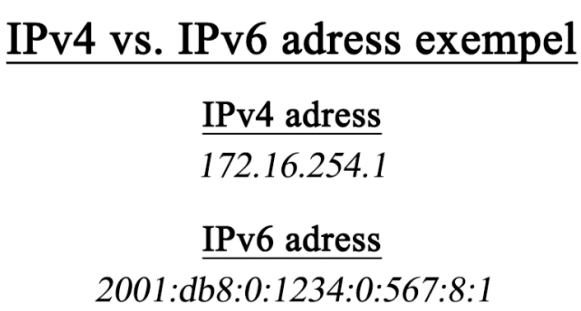
2.3.1 TCP

Överföringskontroll protokollet (eng. *Transmission Control Protocol*, TCP) är ett, som namnet föreslår, överföringsprotokoll som möjliggör två värdar (till exempel två datorer) att etablera en anslutning mellan sig. TCP opererar på transportlagret i

OSI-modellen och till dess uppgifter hör också att se till att alla paket som skickas, värdarna emellan, kommer fram samt att de kommer i rätt ordning (liknande LLCs uppgifter). Detta är den mest signifikanta skillnaden mellan TCP och det mindre pålitliga användardatagramprotokollet (eng. *User Datagram Protocol*, UDP). Allmänt så används TCP mycket mera än UDP så därför kommer denna avhandling inte att gå in på desto mera detalj gällande UDP. Sättet TCP kan garantera att alla paket kommer fram fungerar med hjälp av trevägshandskakning (eng. *three-way handshake*). När en anslutning skall upprättas över TCP så skickar först den värden som vill skapa anslutningen ett så kallat ”huvud” (eng. *header*) med en ”SYN” (synkroniserings) bit satt. Den andra värden svarar på detta med ett ”SYN” tillbaka varpå den första värden skickar ett så kallat ”ACK” (eng. *acknowledgement*) som slutför trevägshandskakningen. Efter att anslutningen upprättats så kan utbyte av data påbörjas. Varje paket som skickas över TCP innehåller ett sekvensnummer samt ett bekräftelsenummer. Dessa nummer gör det lätt att hålla reda på i vilken ordning paketen som mottas skall ordnas och ifall ett nummer fattas så vet man att ett paket förlorats och man kan då be om att få just det paketet skickat till sig på nytt. [10]

2.3.2 IP

Internet protokollet (eng. *Internet Protocol*, IP) har två versioner som används för tillfället, IPv4, som i nuläget är betydligt vanligare, och IPv6, som blir allt vanligare i och med att den aktiva processen att övergå från IPv4 till IPv6 framskrider. I figur 2.2 syns den visuella skillnaden mellan en IPv4 och en IPv6 adress. Eftersom IPv4 i dagsläget är så pass mycket vanligare så kommer denna avhandling endast att gå igenom IPv4 i mera detalj.



Figur 2.2: Jämförelse av IPv4 och IPv6 adress

IP bär ansvaret att levererat så kallade ”datagram” mellan värdar. Datagram kan sägas vara synonymt med paket med skillnaden att ett datagram inte kan notifiera avsändaren om det kommit fram eller ej, det vill säga det kan inte garanteras att datagram kommer fram [11]. En IPv4 adress är 32 bitar lång och består av en nätverks adress och en värd adress [9].

När datagram skickas kan det hända att de måste ta en lång väg igenom diverse routrar, modem och andra noder (något system eller enhet som är anslutet till ett nätverk [12]) för att nå sitt mål. Detta leder till att datagrammen måste kunna passera igenom även om de olika noderna har olika begränsningar på ramstorlekar. Det är då IP:s uppgift att dela upp datagrammen i mindre delar, så kallade fragment, som lätt kan skickas och håller alla begränsningar. Fragmenten får alla sitt eget ”huvud” som innehåller information om avsändare, destination, data och så vidare. Fragmenten behöver inte nödvändigtvis ta samma rutt eftersom de alla har samma unika 16 bitars identifierare i sina huvud. På så sätt kan mottagaren lätt återbygga det ursprungliga datagrammet efter att ha mottagit alla fragment. [9]

3 Allmänt om kryptering och attacker

3.1 Varför är kryptering viktigt?

Alla som i dag äger någon sorts mer eller mindre modern apparat så som en smarttelefon, en bärbar dator eller en surfplatta använder sig av kryptering. Detta är kanske inte något som den vardagliga användaren tänker på, men kryptering finns överallt och den finns där för att den behövs. Om man inte använder sig av kryptering så är all den digitala information man behandlar, skickar, mottar och läser på internet oskyddad. Det kanske inte alltid är så lätt för cybertjuvar att få tag på ens personliga data, men om de får tag på den så vill man utan tvekan vara säker på att man använt sig av kryptering så förövaren inte kan direkt läsa i klartext alla meddelanden, lösenord och så vidare som man skickat över nätverket. Att snappa upp paket som sänds via IEEE 802.11 kallas paket sniffning (eng. *packet sniffing*) och är något som vem som helst på samma nätverk kan göra med hjälp av rätt mjukvara, och om dessa pakets innehåll ej är krypterade kommer personen kunna läsa exakt vad de innehåller.

Man kanske inte anser att alla meddelanden man skickar måste vara krypterade eftersom de inte innehåller något viktigt. Även om det kan vara sant så är alla personliga data, per definition, personliga och därför borde ingen annan utan lov få tillgång till den. Man skickar inte alltid lösenord och bankuppgifter fram och tillbaka men även om man skickar något så oskyldigt som sitt namn, födelsedatum, en adress och så vidare så kan en skicklig person med hjälp av den informationen skapa en ganska bra bild av vem du är, vad du gör, kanske var du bor och liknande. Detta är information som kan användas för diverse olagliga syften så som identitetsstöld och utpressning.

Det finns olika typer av kryptering för olika ändamål. Ofta när man tänker på kryptering tänker man på att någon viss algoritm som krypterat ett meddelande som sedan skickas över internet. Men det finns väldigt många andra användningar så som: lösenord till datorn och PIN-kod på telefonen, vilka inte nödvändigtvis alls har något med internet att göra. Det är alltså också viktigt att se till att information som endast är tillgängligt genom att fysiskt hålla i det, så som bilder som bara finns sparade på en mobiltelefon, också är skyddade. Ett lösenord till datorn eller en PIN-kod på mobiltelefonen skyddar denna information även om någon stjäl apparaten

även om den säkerheten också med tid och tålamod kan brytas genom en metod som kallas råstyrka (eng. *brute force)*. I de kommande kapitlen kommer bland annat råstyrkemetoden, olika krypteringsalgoritmer och ett antal olika typer av attacker att behandlas.

3.2 Symmetrisk kryptering

I detta stycke har [13] använts som referens. Den äldsta typen av kryptering som finns är symmetrisk kryptering. Allmänt inom kryptering så använder man sig av så kallade nycklar för att kryptera och dekryptera data. Till skillnad från asymmetrisk kryptering som använder sig av ett nyckelpar för att kryptera respektive dekryptera data så används inom symmetrisk kryptering samma nyckel för båda operationerna. Symmetriska chiffer kan arbeta endera med stora bitar (eng. c*hunks*) av input data eller med varje bit för sig i serie. Om chiffret i fråga arbetar med stora bitar så kallas det ett blockchiffer (eng. *block cipher*) medan det kallas strömchiffer (eng. *stream cipher*) om det arbetar med varje bit för sig. Den största skillnaden mellan de två olika chiffren är att strömchiffer har energikonsumtions- och prestandafördelar över blockchiffer, men de är också mera sårbara för vissa attacker och används därför oftast endast när prestandans vikt är stor. Blockchiffer är en effektiv metod, om den används på rätt sätt, för att hindar obehöriga att läsa data. Det finns ett väldigt stort antal blockchiffer men de mest välkända och globalt använda är DES (från engelskans *Data Encryption Standard*) och dess ersättare, AES (från engelskans *Advanced Encryption Standard*). Eftersom DES inte längre är relevant och har blivit ersatt av AES kommer denna avhandling inte att behandla DES i detalj.

3.2.1 AES

AES certifierades år 2001 och är det primära chiffret för kryptering av elektroniska data som USA:s regering godkänt för användning. AES har varit en global standard för krypteringsalgoritmer sedan den ersatte den åldrande krypteringsalgoritmen DES [13]. AES algoritmen tar som input: sekvenser av bitsträngar som är 128 bitar långa (ofta kallade block) samt en chiffernyckel som är endera 128, 192 eller 256 bitar lång. Längden av det resulterande outputblocket beror på längden av nyckeln som använts. Om en 128 bitars chiffernyckel använts så kommer output blocket också vara 128 bitar. Samma princip gäller också för de två andra chiffernyckellängderna [14].

Algoritmen börjar med att kopiera inputen till en så kallad tillståndsräcka. Räckan får sedan också en omgångsnyckel adderad till sig varpå tillståndsräckan blir transformerad genom att köras igenom en omgångsfunktion 10,12 eller 14 gånger beroende på chiffernyckellängden. Omgångsfunktionen består av 4 olika transformationer:

- *SubBytes()*: substituera bytes
- *ShiftRows()*: skifta rader
- *MixColumns()*: blanda kolumner
- *AddRoundKey()*: addering av omgångsnyckel

Dessa 4 transformationer körs 9,11 eller 13 gånger, beroende på chiffernyckellängden, efterföljt av en sista körning där *MixColumns()* uteblir. Det resulterande blocket är den krypterade informationen [14].

3.3 Asymmetrisk kryptering

Asymmetrisk kryptering beskrivs väldigt bra av Stallings i [15] som i detta kapitel, med underkapitel, har använts som referens. Asymmetrisk kryptering är en form av kryptering som, till skillnad från symmetrisk kryptering, använder sig av två nycklar istället för en för att kryptera och dekryptera information. Dessa nycklar kallas den privata nyckeln och den publika nyckeln och asymmetrisk kryptering är därför ofta också känt på engelska som *public-key encryption*. Det finns en allmän missuppfattning om att användning av asymmetrisk kryptering skulle vara säkrare än användning av symmetrisk kryptering. Detta är dock inte sant och faktum är att säkerhetsgraden av krypteringen som används beror på längden på nyckeln samt på den mängd arbete som krävs för att genom råstyrka, bryta chiffret. En annan missuppfattning är även att asymmetrisk kryptering skulle ersätta symmetrisk kryptering vilket i nuläget är väldigt osannolikt i och med diverse restriktioner, så som nyckelhantering och signering, som asymmetrisk kryptering har som inte symmetrisk kryptering (åtminstone inte till samma grad) har.

Principen bakom asymmetrisk kryptering är ganska simpel. Metoden fungerar som sagt med hjälp av en privat nyckel och en publik nyckel. Dessa två nycklar är besläktade på ett sådant sätt att om den publika nyckeln har använts för kryptering så kan endast den privata nyckeln dekryptera det meddelandet. Den nyckel som användes för att kryptera meddelandet kan alltså inte användas för att dekryptera

det. Varje mottagare/sändare har alltså sitt eget nyckelpar bestående av en publik och en privat nyckel. Den privata nyckeln hålls hemlig och endast ägaren känner till denna medan den publika nyckeln kan t.ex. publiceras online och distribueras på olika sätt för att vara tillgänglig för i princip alla. Om en sändare vill skicka ett meddelande till en mottagare så behöver sändaren först hämta mottagarens publika nyckel och med hjälp av den, kryptera meddelandet. Som tidigare nämnt så är det endast den besläktade privata nyckeln som kan dekryptera meddelandet och därför kan nu det krypterade meddelandet skickas säkert till mottagaren. Eftersom den privata nyckeln aldrig distribueras så är det endast mottagaren som kan dekryptera meddelandet, så även om någon fick tag på det krypterade meddelandet skulle de inte kunna tolka det.

3.3.1 RSA

Vissa asymmetriska krypteringsalgoritmer så som RSA tillåter kryptering med hjälp av endera den publika nyckeln eller den privata, men endast den andra kan användas för dekryptering. Detta möjliggör att man även kan använda asymmetrisk kryptering för autentisering. Om person A krypterar ett meddelande med sin privata nyckel, så kan person B verifiera att person A verkligen är vem hen säger att hen är, genom att dekryptera meddelandet med person As publika nyckel. Om meddelandet blir klartext efter dekrypteringen så vet person B att person A talar sanning, eftersom endast person A kan ha krypterat meddelandet i fråga. RSA, som har fått sitt namn efter dess utvecklare Ron Rivest, Adi Shamir och Len Adleman, är den mest använda asymmetriska krypteringsalgoritmen.

RSA algoritmen är ett blockchiffer där klartext och chiffertext är heltal mellan 0 och $\boldsymbol{n}$ för något visst $\boldsymbol{n}$ (ofta 1024 bitar). Klartexten omvandlas till krypterade block vars binära värden är mindre än $\boldsymbol{n}$. Kryptering och dekryptering följer följande formler där klartextblocket är $\boldsymbol{M}$ och chiffertextblocket är $\boldsymbol{C}$.

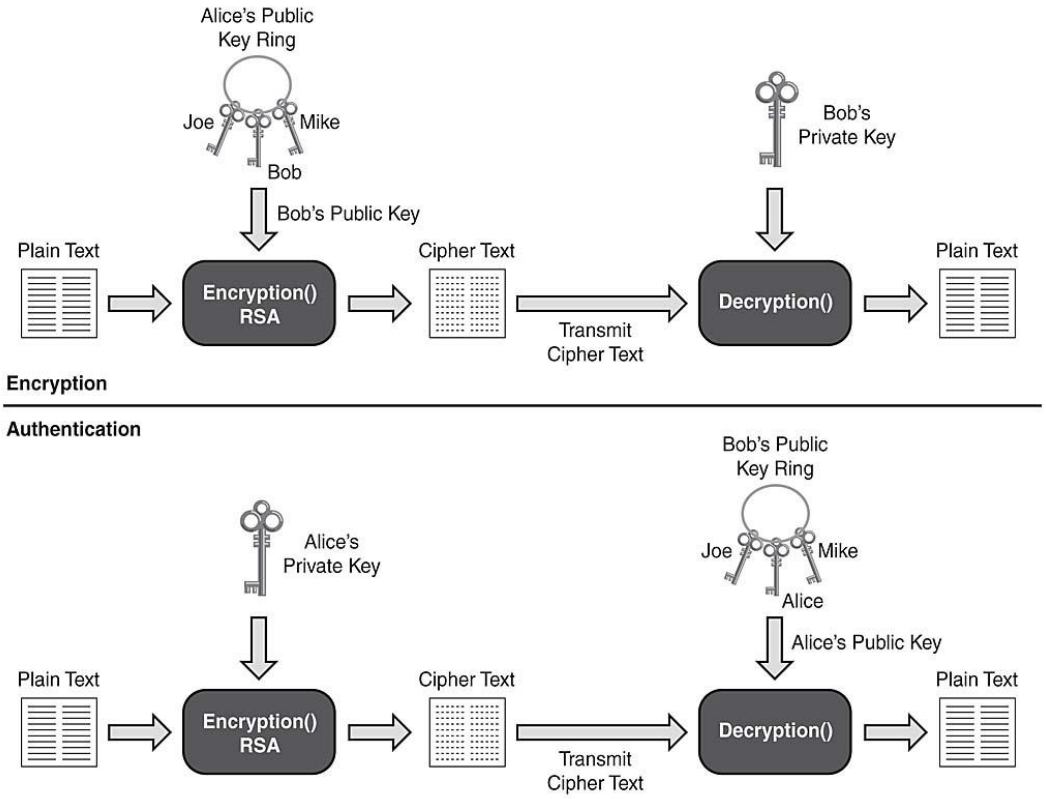
$$\boldsymbol{C} = \boldsymbol{M}^{\boldsymbol{e}} \bmod \boldsymbol{n}$$

$$\boldsymbol{M} = \boldsymbol{C}^{\boldsymbol{d}} \bmod \boldsymbol{n} = (\boldsymbol{M}^{\boldsymbol{e}})^{\boldsymbol{d}} \bmod \boldsymbol{n} = \boldsymbol{M}^{\boldsymbol{ed}} \bmod \boldsymbol{n}$$

Endast mottagaren känner till värdet på $\boldsymbol{d}$ medan sändaren känner till värdet på $\boldsymbol{e}$. Båda parterna känner till $\boldsymbol{n}$ så med andra ord består den publika nyckeln av värdena $\{\boldsymbol{n}, \boldsymbol{e}\}$ och den privata nyckeln består av värdena $\{\boldsymbol{n}, \boldsymbol{d}\}$. Avhandlingen kommer

inte gå in i mera detalj om hur kalkylerna i algoritmen sker men detta är på ett allmänt plan, principerna bakom krypteringsalgoritmen.

Figur 3.1 beskriver hur kryptering, dekryptering samt autentisering går till vid användning av RSA.



Figur 3.1 Visuell beskrivning av kryptering och autentisering med hjälp av RSA [16]

3.4 Att bryta krypteringar

Ett simpelt och välkänt sätt att försöka bryta olika krypteringar är genom råstyrka (eng. *brute-force*). Råstyrkemetoden går ut på att man med hjälp av datorkraft provar dekryptera krypterad information med alla möjliga nycklar ända tills man hittar den nyckel som ger ut klartextversionen av informationen. I medeltal så måste man prova hälften av alla möjliga nycklar innan man hittar den rätta, i värsta fall måste man prova alla. Denna metod förutsätter dock att man vet vilken krypteringsalgoritm som använts för att kryptera innehållet. Dessutom så är metoden väldigt opraktiskt när det så kallade nyckelutrymmet är stort. Nyckelutrymmet är den mängd möjliga nycklar för en given längd på nyckeln. Nyckelutrymmet växer exponentiellt då nyckelns storlek ökar. Tabell 3.1 visar tiden det skulle räcka att bryta krypteringen (för AES och DES) för en dator som

kan göra en miljard dekrypteringar per sekund samt för en dator som kan göra 10^{13} dekrypteringar per sekund [17].

Key Size (bits)	Cipher	Number of Alternative Keys	Time Required at 10^9 Decryptions/s	Time Required at 10^{13} Decryptions/s
56	DES	$2^{56} \approx 7.2 \times 10^{16}$	2^{55} ns = 1.125 years	1 hour
128	AES	$2^{128} \approx 3.4 \times 10^{38}$	2^{127} ns = 5.3×10^{21} years	5.3×10^{17} years
168	Triple DES	$2^{168} \approx 3.7 \times 10^{50}$	2^{167} ns = 5.8×10^{33} years	5.8×10^{29} years
192	AES	$2^{192} \approx 6.3 \times 10^{57}$	2^{191} ns = 9.8×10^{40} years	9.8×10^{36} years
256	AES	$2^{256} \approx 1.2 \times 10^{77}$	2^{255} ns = 1.8×10^{60} years	1.8×10^{56} years
26 characters (permutation)	Monoalphabetic	$2! = 4 \times 10^{26}$	2×10^{26} ns = 6.3×10^{9} years	6.3×10^{6} years

Tabell 3.1 Tid som i medeltal krävs för att hitta rätt nyckel för olika chiffer. [18]

Det är också möjligt att genom råstyrkemetoden bryta RSA-krypterade data, men i praktiken är det ofta opraktiskt. Ju flera antal bitar variabeln ***d*** i figur 3.1 består av, desto säkrare är krypteringen. Det leder dock också till att på grund av kalkyleringarna som ingår i både kryptering och dekryptering, kommer systemet som utför dem behöva mer tid för uträkningarna [15].

3.5 Attacker över IEEE 802.11

Vid användning av både IEEE 802.11 och Ethernet löper man en risk att bli utsatt för diverse attacker. Detta kapitel kommer kort gå igenom ett antal attacker som man kan bli utsatt för speciellt vid användning av IEEE 802.11.

3.5.1 Överbelastningsattacker

En överbelastningsattack är en attack där attackeraren med någon metod överbelastar offret, till exempel en router, på ett sådant sätt att det inte längre kan fungera som det ska. Majoriteten av alla överbelastningsattacker (eng. *denial-of-service*, DoS) över IEEE 802.11 uppkommer från sårbarheter i så kallade hanteringsramar (eng. *management frames*) som inte är skyddade av något 802.11 protokoll [19]. Hanteringsramar är en typ av ramar som utför övervakningsfunktioner. De används till att gå med i och lämna trådlösa nätverk, och även för att flytta associationer från en åtkomstpunkt till en annan [20]. Till följande tas upp tre olika typer av DoS-attacker som kan åstadkommas genom att utnyttja sårbarheten av hanteringsramar.

En avautentiseringsöverbelastningsattack (eng. D*eauthentication Flooding*, DeAuthF) är en attack där förövaren kontinuerligt skickar avautentiseringsramar till offret för att göra det oåtkomligt för andra klienter på nätverket. Avautentisering är en så kallad avisering och sådana kan inte ignoreras av klienter och därför måste mottagaren, i det här fallet offret, implementera sin funktion för att koppla bort sig från nätverket. I värsta fall så är åtkomstpunkten offret och i så fall blir alla klienter som är anslutna till nätverket otillgängliga [19].

Överbelastning genom autentiseringsförfrågningar (eng. *Authentication Request Flooding*, AuthRF) är en typ av attack som utförs genom att attackeraren använder sig av en falsk MAC-adress och skickar en autentiseringsbegäran till åtkomstpunkten. Åtkomstpunkten svarar då med ett autentiseringssvar, men eftersom det inte finns någon enhet med den falska MAC-adressen så kommer svaret aldrig fram och åtkomstpunkten får aldrig den bekräftelse den väntar på. Åtkomstpunkten kommer då att igen och igen skicka samma svarsram vilket kommer att överbelasta dess resurser. Detta leder till att åtkomstpunkten har väldigt lite resurser kvar för att delge andra trådlösa klienter och de kan då i sin tur hamna ut för dålig kommunikationsförmåga eller helt och hållet tappa kommunikationen [19].

Åtkomstpunkter håller koll på alla associerade enheter genom att hålla en associationstabell i minnet. Denna tabell skrivs till när åtkomstpunkten tar emot en associationsbegäran av en klient. Tabellens maximala storlek är 2007 associationer, per IEEE 802.11 standard. En överbelastningsattack genom associationsbegäranden (eng. *Association Request Flooding*, AssRF) utnyttjar detta faktum genom att med många olika förfalskade MAC-adresser, skicka associationsbegäranden till åtkomstpunkten. Åtkomstpunkten kommer då att fylla sin tabell med dessa falska MAC-adresser och efter att tabellen fyllts kommer den inte längre acceptera nya associationer. Denna attack förutsätter dock att förövaren redan innan fått tag på lösenordet till IEEE 802.11 nätverket [20].

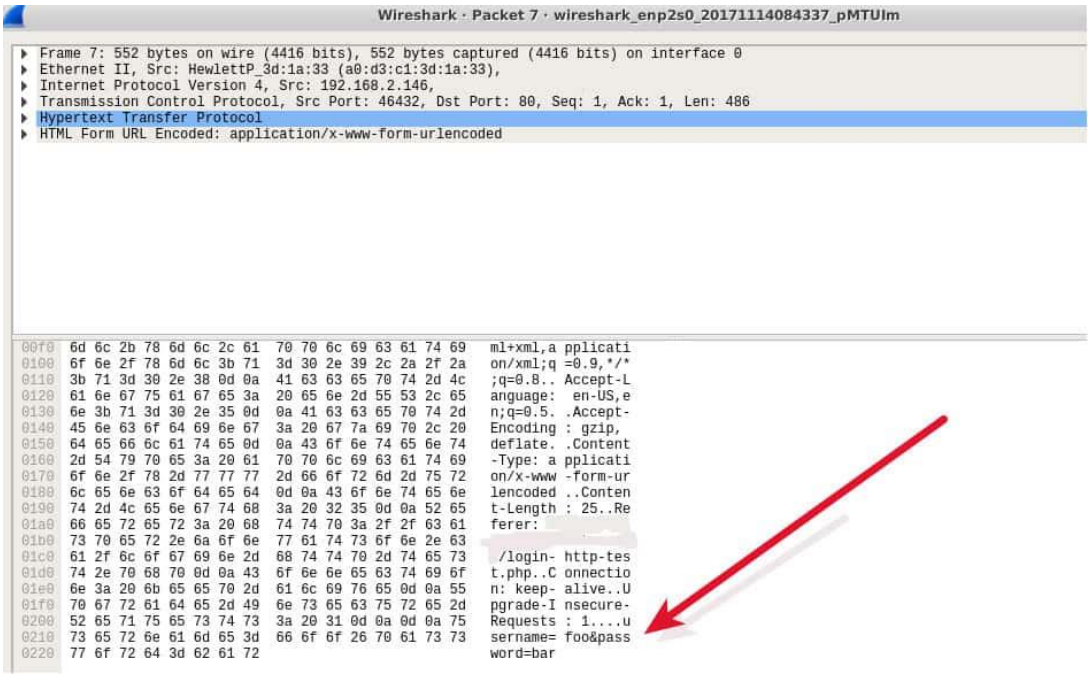
3.5.2 Paketsniffning

Paketsniffare är mjukvara som används som endera administrativa verktyg eller verktyg för olagliga syften, beroende på användarens avsikter. Dessa program snappar upp paket som skickas över TCP/IP och tolkar dem [4]. Packetsniffning är

inte direkt en attack men beroende på avsikt och vem som gör det kan det ses som en attack mot den personliga integriteten. Man brukar kalla paketsniffning med illegala avsikter för ”passiva attacker” eftersom attackeraren inte direkt ansluter till något annat system på nätverket [21]. Paketsniffare används både över Ethernet anslutningar och IEEE 802.11 men eftersom man högst sannolikt använder sig av IEEE 802.11 när man ansluter sig till publika nätverk och inte av fast anslutning, så är det relevant att nämna hur de fungerar.

Nästan vem som helst kan få tillgång till ett offentligt nätverk, till exempel på ett café, och det betyder alltså också att vem som helst som anslutit sig till nätverket kan använda sig av en paket sniffare för att få tag på andra användares känsliga information. När man pratar om känslig information menar man ofta användarnamn, lösenord och annan konfidentiell information.

Det finns en handfull protokoll som är sårbara för packetsniffning eftersom deras överföringar inte är krypterade. Bland dessa är HTTP (eng. *Hypertext Transfer Protocol*), FTP (eng. *File Transfer Protocol*) och ett antal mejl-protokoll de vanligaste [21]. Många av dessa har dock versioner som använder kryptering, till exempel HTTPS (eng. *Hypertext Transfer Protocol Secure*), vilket gör dem säkrare mot paketsniffare. Oberoende om paketen är krypterade eller ej så kan paketsniffare snappa upp dem, skillnaden är förstås att om de är krypterade så är de inte direkt läsliga som klartext vilket de vore om de inte var krypterade. Figur 3.1 visar en skärmdump av paketsniffningsmjukvaran *Wireshark* som snappat upp ett paket som innehåller HTTP-innehåll. Längst ner ser man klart och tydligt både användarnamn och lösenord i klartext.



Figur 3.1 Skärmdump av ett uppsnappat paket i Wireshark [22].

4 Säkerhetsmekanismer i IEEE 802.11

Hittills har avhandlingen gått igenom hur IEEE 802.11 fungerar och dess risker. Trots dessa risker så är man i dagens samhälle nästan tvungen att använda sig av IEEE 802.11. Därför är det också viktigt att veta vad man bör tänka på för att hålla sig så säker som möjligt och hur man kan själv optimera det egna IEEE 802.11 nätverket för att bibehålla säkerheten.

I Jason S. Kings tekniska rapport [23] beskrivs säkerhetsmekanismerna som IEEE 802.11 använder sig av. Kings rapport har i detta kapitel använts som referens för SSID, Autentisering och WEP.

4.1 SSID

SSID (från engelskans *Service Set Identifier*) är IEEE 802.11 nätverkets namn utåt. Det identifierar unikt nätverket och skiljer det från andra nätverk som också är inom räckhåll. Består nätverket av flera åtkomstpunkter så bör de alla ha samma SSID, annars identifieras de som skilda nätverk.

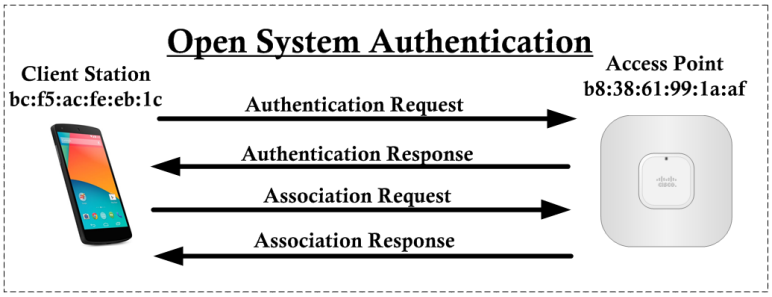
Som standard så sänder åtkomstpunkten i perioder ut sitt SSID i en så kallad *beacon*. En trådlös klient, till exempel en mobiltelefon, som vill ansluta till ett nätverk lyssnar då på dessa sändningar och kan på basis av de *beacons* den sett, välja ett nätverk att ansluta till.

Som en säkerhetsmekanism så kan åtkomstpunkten konfigureras så att den inte sänder ut denna *beacon*. Åtkomstpunkten förblir då osynlig för trådlösa klienter och klienterna måste redan känna till nätverkets SSID för att kunna ansluta genom att ange det manuellt. Om en klient försöker ansluta till en åtkomstpunkt med ett SSID som inte matchar åtkomstpunktens SSID så kommer associationsbegäran att avslås.

Även om den ovannämnda säkerhetsmekanismen är säkrare än att låta åtkomstpunkten sända ut sitt SSID åt alla så erbjuder denna mekanism inte tillräcklig säkerhet. Som tidigare förklarat i kapitlet om paketsniffning så kan en förövare sitta och sniffa upp paket som skickas i närheten. Ett av dessa paket som förövaren kan få tag på kan innehålla den dolda åtkomstpunktens SSID i ett av de tidigare nämna hanteringsfönstren som används för att associera med och lämna trådlösa nätverk.

4.2 Autentisering

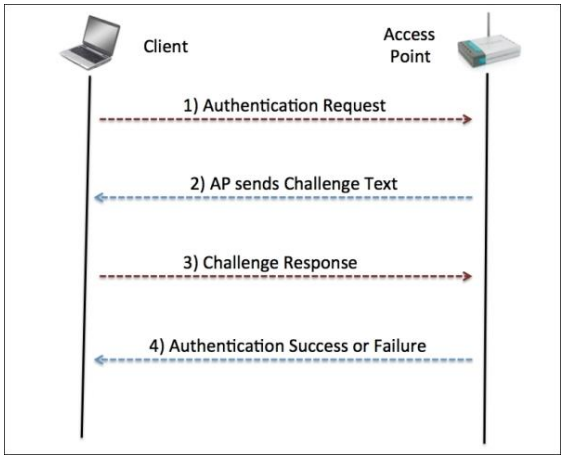
Inom IEEE 802.11 så finns det två typer av autentisering: öppen och autentisering med delad nyckel. Processen som genomgås vid öppen autentisering är väldigt simpel och åskådliggörs i figur 4.1. Öppen autentisering är alltså kort sagt när ett IEEE 802.11 nätverk är konfigurerat på ett sådant sätt att det inte begär ett lösenord vid associering och alltid svarar positivt på autentiseringsbegäranden.



Figur 4.1 Processen vid öppen autentisering. [24]

Grundprincipen för autentisering med delad nyckel är att båda parterna, det vill säga åtkomstpunkten och den trådlösa klienten, båda använder samma nyckel. Denna nyckel är ofta delad genom att manuellt ange den i säkerhetsinställningarna för åtkomstpunkten samt vid associationsprocessen på klientsidan.

Skillnaden mellan öppen autentisering och autentisering med delad nyckel åskådliggörs i figur 4.2. Då klienten begär att autentisera sig med åtkomstpunkten så svarar åtkomstpunkten med en utmaningstext som klienten bör kryptera med hjälp av den delade nyckeln. Klienten skickar då tillbaka den krypterade texten och om svaret matchar åtkomstpunktens kryptering av utmaningstexten så lyckas autentiseringen.



Figur 4.2 Processen vid autentisering med delad nyckel [25]

4.2.1 WEP

WEP (eng. *Wired Equivalent Privacy*) är ett säkerhetsprotokoll som specificerades i IEEE 802.11b standarden. Det används både vid kryptering av data och autentisering.

Det verkar som att autentisering med delad nyckel, som nämndes i föregående kapitel, skulle vara det säkraste autentiseringsalternativet, men detta är inte sant när det gäller autentisering med WEP. Autentisering med delad nyckel och WEP bär en säkerhetsrisk som baserar sig på att vem som helst kan genom paketsniffning få tag på den icke krypterade utmaningstexten som åtkomstpunkten skickar till klienten samt den det krypterade svaret som klienten svarar med. På basis av dessa två kan förövaren räkna ut den delade nyckeln. På grund av detta så är det bästa alternativet att använda öppen autentisering tillsammans med WEP eftersom även om vem som helst kan autentisera sig så kommer åtkomstpunkten att blockera all trafik till och från klienter som inte har rätt WEP-nyckel.

WEP är numera föråldrat och borde inte användas på grund av diverse säkerhetsproblem med till exempel längden på nycklarna som med dagens datorkraft lätt kan räknas ut med hjälp av den tidigare nämna råstyrkemetoden. WEP blev officiellt ersatt av WPA år 2004 [26].

4.2.2 WPA, WPA2 och WPA3

WPA (eng. *Wi-Fi Protected Access*) utvecklades för att överkomma de sårbarheter som WEP medförde och dök först upp på marknaden 2003. Dess funktionalitet beskrivs av Steve Rackley i [27].

WPA använder sig av det temporära nyckel integritetsprotokollet (eng. *temporal key integrity protocol*, TKIP). WPA erbjuder också ett val mellan två olika autentiseringsmetoder: det sträckbara autentiseringsprotokollet (eng. *extensible authentication protocol*, EAP) som främst riktar sig åt företag, eller en enklare metod som använder sig av en fördelad nyckel (eng. *pre-shared key,* PSK) som är ämnad för hemmaanvändning eller mindre kontor.

År 2004 släpptes en förbättrad version av WPA, WPA2, som istället för det gamla krypteringschiffret, RC4, använder sig av AES som är betydligt säkrare. I moderna routrar och modem får man själv välja säkerhetsläge och krypteringschiffer. Alternativen för lägen är ofta mellan WPA/WPA2 eller endast WPA2 och AES eller

AES+TKIP för krypteringschiffren. Valet som görs är beroende på vilka chiffer och krypteringsmetoder klienterna som skall ansluta sig till IEEE 802.11 nätverket stöder.

Den allra senaste versionen av WPA är dock inte WPA2 utan WPA3 har nu utvecklats. WPA3 kommer med ett flertal säkerhetsförbättringar och förbättrade skydd mot attacker. WPA2 är ännu den populäraste versionen av WPA eftersom utbudet på WPA3 routrar och modem ännu är litet. Dessutom så behöver de trådlösa klienterna också stöda WPA3 för att fungera tillsammans med åtkomstpunkten som använder sig av WPA3.

4.3 Hur kan användaren upprätthålla säkerheten?

Den här avhandlingen har hittills tagit upp en del potentiella hot mot säkerheten inom IEEE 802.11 samt en del säkerhetsmekanismer som IEEE 802.11 använder sig av. Dessa hot och mekanismer gäller för alla, både hemma användare och företag, som använder sig av IEEE 802.11. I detta kapitel tas det upp hur en användare kan upprätthålla säkerheten på sitt IEEE 802.11 nätverk hemma så effektivt som möjligt. Kapitlet igenom antas det att användaren har vetskap om hur man får tillgång till åtkomstpunktens inställningar.

4.3.1 Håll mjukvaran och hårdvaran uppdaterad

Mjukvaran och brandväggen som kommer färdigt installerade på IEEE 802.11 åtkomstpunkten när man köper den är inte perfekta och vissa åtkomstpunkter kanske till och med saknar brandvägg. Därför krävs uppdateringar när buggar och kryphål i säkerheten hittas. Man kan i åtkomstpunktens inställningar ofta hitta någon form av fast programuppdateringsfunktion (eng. *firmware update*) som låter användaren manuellt uppdatera mjukvaran i sin enhet till den allra senaste som förhoppningsvis fixar alla säkerhetsproblem som hittats sedan den förra uppdateringen. Tyvärr så händer det ofta att tillverkare slutar skicka ut uppdateringar till aningen äldre enheter vartefter de släpper ut nyare modeller. Detta leder till att användaren av en äldre enhet inte längre får de senaste säkerhetsuppdateringarna och därför nästintill tvingas köpa en nyare modell för att hålla takten. Tillverkarna anger ofta en livscykel för sina produkter och när den gått ut och produkten inte längre får nya uppdateringar borde användaren överväga att införskaffa en ny, även om den gamla fortfarande fungerar som den ska.

4.3.2 Ändra uppgifterna för administratörkontot

Innan man kan börja tänka på att ställa in ett lösenord och kryptering för sin åtkomstpunkt bör man se till att ändra uppgifterna för det förinställda administratörkontot för enheten. Dessa uppgifter är ofta angivna på undersidan av enheten och är också ofta identiska för tillverkarens samtliga åtkomstpunkter och kan lätt hittas på internet. Detta betyder att om man inte ändrar dem så kan vem som helst som är ansluten till IEEE 802.11 nätverket också lätt logga in och ändra inställningar för enheten. Det är därför viktigt att se till att ändra dessa uppgifter innan man börjar konfigurera andra inställningar eftersom det är ingen poäng att optimera säkerheten om sedan vem som helst kan ta bort inställningarna.

4.3.3 Konfigurera autentisering

Efter att administratörkontots uppgifter har ändrats borde användaren ställa in någon form av autentisering. Exempel på olika autentiseringstyper togs upp i kapitel 4.2. I åtkomstpunktens inställningar kan användaren konfigurera vilket säkerhetsläge, kryptering samt lösenfras som ska användas. Det bästa är att välja den senaste versionen av WPA som enheten och alla klienter i nätverket stöder. Om valet är mellan ”WPA/ WPA2” och ”Endast WPA2” så är det senare alternativet det säkrare eftersom enheten då inte använder sig alls av de föråldrade osäkra funktionerna av WPA. Valet beror dock också som sagt på klienterna i nätverket och vad de stöder. Krypteringen beror på vilket val av säkerhetsläge man gjort men ofta har man valet mellan AES och AES+TKIP. Igen så beror det på klienterna men det säkrare alternativet är AES eftersom AES+TKIP är endast där för att stöda både AES och äldre enheter med TKIP. Gällande lösenfrasen så borde den vara relativt lång och slumpmässigt vald för att vara så säker som möjligt. Ofta väljer användare dock att ha något som är lätt att komma ihåg, vilket inte är det säkraste men det är upp till var och en att bestämma vilken blandning av bekvämhet och säkerhet man vill ha.

Om man är riktigt noga med säkerheten, och har en router som stöder det, så kan man konfigurera den att använda sig av företagsversionen av valt säkerhetsläge (eng. *WPAx-Enterprise*, där x är den valda versionen av WPA). Vid användning av detta läge har varje klient i nätverket ett eget användarnamn och lösenord som de loggar in med. De har också sin egen krypteringsnyckel så de kan endast se sin egen trafik och inte någon annans.

4.3.4 Dölj åtkomstpunktens SSID

Som tidigare nämnt i kapitel 4.1 så är åtkomstpunkter från början konfigurerade att sända ut sitt SSID så att klienter lätt kan hitta den och ansluta. Denna funktion kan också som sagt stängas av för att höja säkerheten. När funktionen är avstängd så kan klienterna inte se åtkomstpunkten utan de måste manuellt ange SSID:t samt lösenfras när de ansluter. För vanliga användare är detta ofta tillräckligt för att hindra att obehöriga ens försöker ansluta till nätverket men för användare med lite mera kunskap så är det ändå inga större problem att få tag på SSID:t genom till exempel sniffning. Därför borde denna funktion endast använda som ett sätt att främja säkerheten och bör inte vara en avgörande faktor för säkerheten som helhet.

4.3.5 MAC-filtrering

En annan funktion som kan främja säkerheten, men som inte heller borde litas på allt för mycket, är MAC filtrering. De flesta åtkomstpunkter har en inbyggd funktion som tillåter administratören av IEEE 802.11 nätverket att ange en lista med MAC-adresser som tillåts ansluta till nätverket. Alla enheter vars MAC-adresser inte finns på denna lista tillåts inte ansluta, även om de skull ange korrekt lösenfras.

En användare med kunskap om hur man använder en falsk MAC-adress kan dock lätt undgå detta filter. Genom sniffning kan förövaren få reda på en MAC-adress som tillåts ansluta. Förövaren kan då lura åtkomstpunkten genom att använda sig av denna MAC-adress för att ansluta till nätverket.

För ett vanligt hemmanätverk kan användningen av MAC-filtrering höja säkerheten, men borde inte vara en avgörande faktor.

4.3.6 Stäng av WPS

WPS (eng. *Wi-Fi Protected Setup*) är en funktion som många åtkomstpunkter har nu för tiden. Funktionen tillåter klienter att ansluta till nätverket genom att använda en kortare PIN-kod, bestående av endast siffror, istället för lösenfrasen som högst antagligen är både längre och betydligt mera komplicerad.

Denna funktion, som ofta kommer aktiverad från början, låter som ett behändigt sätt för en klient att ansluta men öppnar också upp för en betydligt lättare råstyrkeattack för en förövare. På grund av att längden på PIN-koden är kortare och förövaren endast behöver testa siffror förminskas arbetet som råstyrkeattacken måste utföra radikalt. WPS har dock en säkerhetsmekanism som endast tillåter ett

visst antal felaktiga PIN-koder innan den stänger av WPS helt och hållet. Men även denna funktion kan manipuleras eftersom den återställs ofta när åtkomstpunkten startas om, vilket kan tvingas genom att förövaren genomför någon form av överbelastningsattack.

Denna funktion är med andra ord väldigt sårbar mot råstyrkeattacker och för att förbättra säkerheten borde den stängas av i åtkomstpunktens inställningar.

4.3.7 Ändra åtkomstpunktens IP-adress

Som nämnt i början av kapitlet så antas i kapitel 4.3 att användaren har vetskap om hur man får tillgång till åtkomstpunktens inställningar. Detta sker alltså genom att ange åtkomstpunktens IP-adress i en webbläsare och logga in med administratörkontot. Denna IP-adress är dock väldigt ofta identisk för många åtkomstpunkter vilket gör det lätt för vem som helst som är ansluten till nätverket att åtminstone nå inloggningssidan. Följande adresser är bland de allra vanligaste IP-adresserna för åtkomstpunkter:

- *192.168.1.1*
- *192.168.0.1*
- *192.168.2.1*

Ett sätt att vidare höja säkerheten och hindra att obehöriga ens försöker logga in och ändra i åtkomstpunktens inställningar vore att ändra denna IP-adress. Detta försvårar arbetet för potentiella förövare eftersom de nu först måste ta reda på åtkomstpunktens IP-adress innan de kan påbörja till exempel en råstyrkeattack mot inloggningssidan.

4.3.8 Användarens säkerhetschecklista

För att kort sammanfatta vad användaren kan göra för att höja säkerheten på sitt eget IEEE 802.11 nätverk finns nedan en checklista. Punkterna på checklistan framkommer i samma ordning som de tagits upp ovan i detta kapitel.

- Se till att både mjukvara liksom hårdvara är uppdaterad för att få tillgång till de senaste säkerhetsförbättringarna
- Ändra lösenord (och möjligtvis användarnamn) för administratörkontot för att förhindra obehörig åtkomst till åtkomstpunktens inställningar
- Ställ in någon form av autentisering (gärna med WPA2 eller senare)

- Dölj åtkomstpunktens SSID så att endast användare som känner till SSID:t kan ansluta
- Använd MAC-filtrering för att endast tillåta valda enheter att ansluta
- Stäng av WPS för åtkomstpunkten för att inte vara sårbar för WPS-relaterade råstyrkeattacker
- Ändra åtkomstpunktens förvalda IP-adress för att försvåra åtkomsten till åtkomstpunktens inställningar för obehöriga

5 Sammanfattning

När jag började skriva på denna avhandling visste jag ärligt talat inte vad IEEE 802.11 var för något. Förstås kände jag till termen ”wifi” men jag visste inte att den termen egentligen bara är ett handelsnamn för teknik som baserar sig på IEEE 802.11 standarder. Historian bakom IEEE 802.11 var något helt nytt för mig och jag hade aldrig vetat vad skillnaderna på de olika versionerna av 802.11 var. För mig personligen är 5GHz-teknik relativt modernt, vilket ledde till en stor förvåning när jag fick reda på att tekniken i grund och botten funnits nästan sedan början av IEEE 802.11 standarderna, även om dess användning då ansågs opraktisk.

Innan jag skrev denna avhandling var jag ytligt insatt i vilka hot som användningen av IEEE 802.11 medförde, men genom läsning av referensmaterialet har jag nu en mycket bättre bild av hur olika processer egentligen går till. Samma sak gällde kryptering, jag visste grundprinciperna bakom det men inte hur de olika typerna skilde sig från varandra eller vad deras för- respektive nackdelar var. Det var fascinerande att få läsa om hur symmetrisk och asymmetrisk kryptering fungerar och varför den ena borde användas över den andra i vissa situationer. Det är för mig nu mera klart varför asymmetrisk kryptering, även metoden är yngre, inte direkt är bättre än symmetrisk kryptering. Det finns ingen kryptering som man i dagsläget kan säga att med all säkerhet ej kan brytas, om inte nu så i framtiden. Enligt mig är kryptering i en konstant kapplöpning med datorkraft och cyberattacker. För vår, användarnas, skull hoppas jag verkligen att kryptering och säkerhet alltid har ett försprång.

Alla attacker handlar dock inte om att bryta krypteringar, speciellt om där inte finns någon kryptering. I dessa fall gäller det att vara aktsam med vilka sidor man besöker, vilken information man delar och på vilka nätverk man gör det. Man bör se till att alltid använda kryptering när det är möjligt och aldrig hantera känslig information på IEEE 802.11 nätverk vars säkerhet och användare är okända.

Vi kan aldrig vara helt säkra när vi använder internet, men vi bör göra vårt bästa för att vara så säkra som möjligt för att minska potentiella hot och risker vi kan utsättas för. Det är därför alltid allra bekvämast att så ofta som möjligt använda sig av det egna bekanta IEEE 802.11 nätverket som man har hemma, istället för ett offentligt nätverk. Hemma har vi själv kontroll över nätverket och kan själva konfigurera det

att använda så många säkerhetsmekanismer som vi anser oss behöva för att känna oss så trygga som möjligt. När det gäller säkerhet över IEEE 802.11 kan vi inte annat än att göra vårt bästa för att upprätthålla den och följa med utvecklingen i hopp om att i framtiden få se ett nästintill ogenomträngligt IEEE 802.11.

Referenser

[1] J. Stevens, ”Internet Stats & Facts for 2019,” 17 December 2018. [Online]. Available: https://hostingfacts.com/internet-facts-stats/. [Använd 2 Februari 2019].

[2] P. Christensson, ”RJ45 Definition,” TechTerms, 1 Juli 2011. [Online]. Available: https://techterms.com/definition/rj45. [Använd 2 Februari 2019].

[3] ”Wi-Fi Alliance,” Wi-Fi Alliance, [Online]. Available: https://www.wi-fi.org/who-we-are/history. [Använd 2 Februari 2019].

[4] S. Ansari, S. G. Rajeev och H. S. Chandrashekar, ”Packet sniffing: a brief introduction,” *IEEE Potentials,* vol. 21, nr 5, pp. 17-19, Dec 2002/Jan 2003.

[5] M. Rouse, ”Techtarget: SearchMobile Computing,” November 2006. [Online]. Available: https://searchmobilecomputing.techtarget.com/definition/80211. [Använd 4 Februari 2019].

[6] J. Kim och I. Lee, ”802.11 WLAN: history and new enabling MIMO techniques for next generation standards,” *IEEE Communications Magazine,* vol. 53, nr 3, pp. 134-140, 2015.

[7] R. Shimonski, ”OSI Model,” i *Network+ Study Guide & Practice Exams*, Elsevier, 2005, pp. 247-315.

[8] ”Wikipedia,” [Online]. Available: https://sv.wikipedia.org/wiki/OSI-modellen#/media/File:OSI_Model_v1.svg. [Använd 5 Februari 2019].

[9] S. Mackay, E. Wright, D. Reynders och J. Park, ”TCP/IP overview,” i *Practical Industrial Data Networks*, Elsevier, 2004, pp. 257-276.

[10] W. Goralski, ”Transmission Control Protocol,” i *The Illustrated Network (Second Edition)*, Elsevier, 2017, pp. 307-329.

[11] P. Christensson, ”Datagram Definition,” TechTerms, 22 September 2016. [Online]. Available: https://techterms.com/definition/datagram. [Använd 20 Februari 2019].

[12] P. Christensson, ”Node Definition,” TechTerms, 2006. [Online]. Available: https://techterms.com/definition/node. [Använd 20 Februari 2019].

[13] T. J. Shimeall och J. M. Spring, ”Resistance Strategies Symmetric Encryption,” i *Introduction to Information Security*, Elsevier, 2014, pp. 159-175.

[14] *Announcing the Advanced Encryption Standard (AES),* National Institute of Standards and Technology (NIST), 2001.

[15] W. Stallings, ”Chapter 9. Public-Key Cryptography and RSA,” i *Cryptography and Network Security Principles and Practices, Fourth Edition*, Prentice Hall, 2005, pp. 257-262, 268-270, 275.

[16] Q. Huang och J. Frahim, ”Network World,” 2 Oktober 2008. [Online]. Available: https://images.techhive.com/images/idge/imported/article/nww/2008/10/02fig02-100277994-orig.jpg. [Använd 12 Mars 2019].

[17] W. Stallings, ”Cryptanalysis,” i *Cryptography and Network Security Principles and Practices, Fourth Edition*, Prentice Hall, 2005, pp. 32-35.

[18] W. Stallings, ”Table 3.5: Average Time Required for Exhaustive Key Search,” i *Cryptography and Network Security: Principles and Practices, Sixth Edition*, Pearson, 2014, p. 78.

[19] M. Malekzadeh, A. A. A. Ghani, J. Desa och S. Shamala, ”An Experimental Evaluation of DoS Attack and Its Impact on Throughput of IEEE 802.11 Wireless Networks,” *International Journal of Computer Science and Network Security,* vol. 8, nr 8, 2008.

[20] T. Farooq, D. Llewellyn-Jones och M. Merabti, ”MAC Layer DoS Attacks in IEEE 802.11 Networks,” Januari 2010. [Online]. Available: https://www.researchgate.net/publication/266467295_MAC_Layer_DoS_Attacks_in_IEEE_80211_Networks. [Använd 18 Mars 2019].

[21] M. Krishnamurthy, E. S. Seagren, R. Alder, A. W. Bayles, J. Burke, S. Carter och E. Faskha, ”Network Analysis, Troubleshooting, and Packet Sniffing,” i *How to Cheat at Securing Linux*, Elsevier, 2008, pp. 207-209.

[22] W. Jon, ”Comparitech,” 20 Juni 2018. [Online]. Available: https://cdn.comparitech.com/wp-content/uploads/2017/11/Wireshark-NoVPN-HTTP.jpg. [Använd 19 Mars 2019].

[23] J. King, ”IEEE 802.11 Wireless LAN Security White Paper,” 22 Oktober 2001. [Online]. Available: https://www.osti.gov/biblio/15005940. [Använd 21 Mars 2019].

[24] Nayarasi, ”CWSP-Legacy 802.11 Security,” 19 Augusti 2014. [Online]. Available: https://mrncciew.files.wordpress.com/2014/08/cwsp-wep-01.png. [Använd 21 Mars 2019].

[25] ”Shared Key Authentication,” [Online]. Available: https://static.packt-cdn.com/products/9781783280414/graphics/0414OS_03_13.jpg. [Använd 22 Mars 2019].

[26] G. Phillips, ”WEP vs. WPA vs. WPA2 vs. WPA3: Wi-Fi Security Types Explained,” 16 Januari 2019. [Online]. Available: https://www.makeuseof.com/tag/wep-wpa-wpa2-wpa3-explained/. [Använd 22 Mars 2019].

[27] S. Rackley, ”Wireless lan security,” i *Wireless Networking Technology*, Elsevier, 2007, pp. 212-214.